

Exhibit 2



All Our stories Reviews Multimedia **Security Watch**

Cyber Analytics

SECURITY WATCH / SECURITY WATCH



Spammergate: The Fall of an Empire

06 / 03 / 2017

Spammergate: The Fall of an Empire

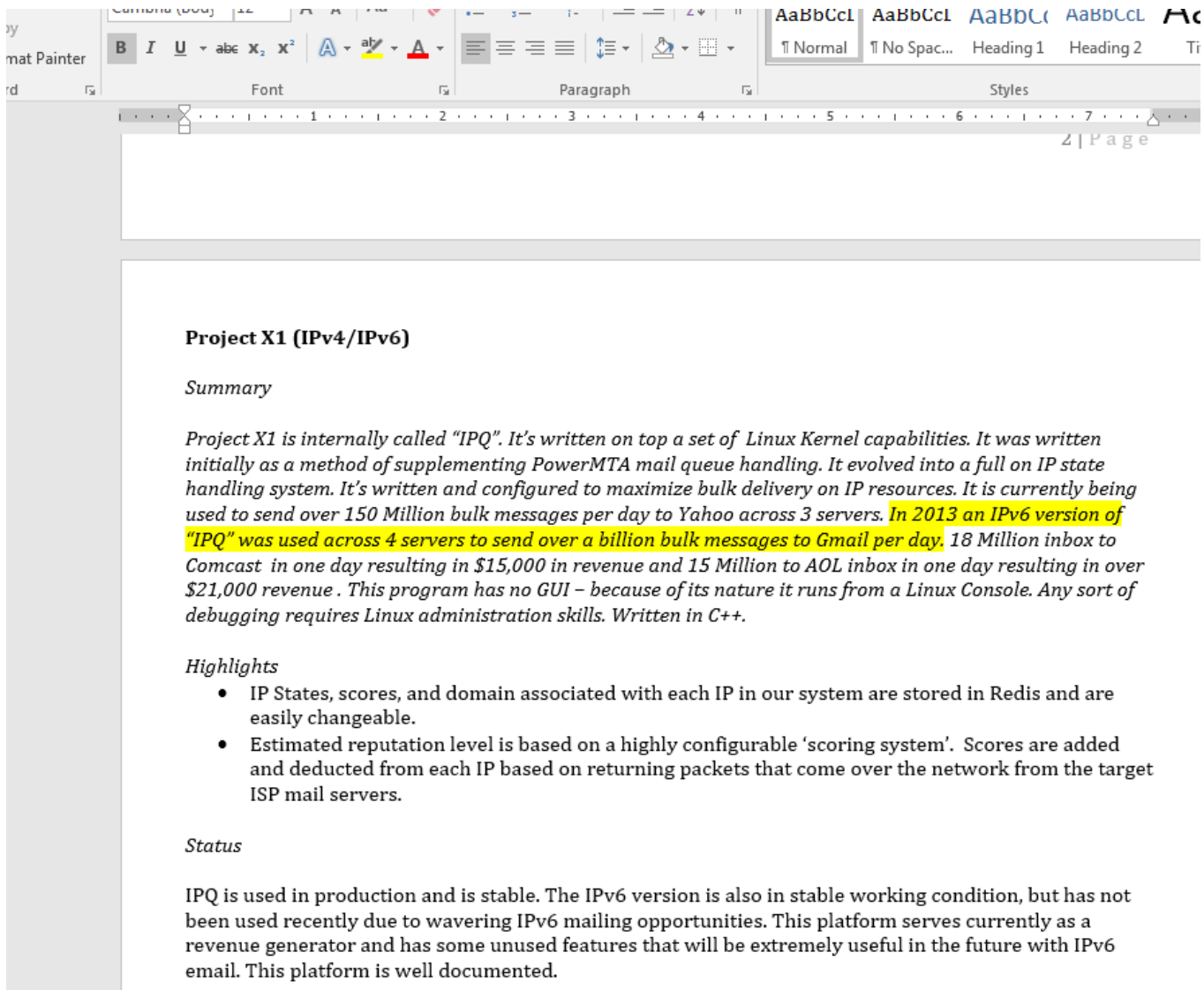
Today we release details on the innerworkings of a massive, illegal spam operation. The situation presents a tangible threat to online privacy and security as it involves a database of 1.4 billion email accounts combined with real names, user IP addresses, and often physical address. Chances are that you, or at least someone you know, is affected.

	A	B	C	D	E	F	G	H	I	J
	Email	First Name	Last Name	IP	Address	City	State	Zip	Country	Note
1	[REDACTED]@yahoo.com	roosevelt	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	fl	33311	US	netfli
2	[REDACTED]@cs.com	yan	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	nj	8527	US	stude
3	[REDACTED]@netscape.net	jeff	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	ca	94574	US	expe
4	[REDACTED]@aol.com	candace	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	wi	53168	US	newe
5	[REDACTED]@worldnet.att.net	gary	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	nc	28645	US	www
6	[REDACTED]@cfl.rr.com	logan	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	va	20180	US	netfli
7	[REDACTED]@yahoo.com	samantha	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	ky	41018	US	www
8	[REDACTED]@yahoo.com	bobbie jo	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	oh	45011	US	expe
9	[REDACTED]@yahoo.com	amanda	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]			US	yourg
10	[REDACTED]@msn.com	jennifer	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	ny	11784	US	123fr
11	[REDACTED]@netscape.net	craig	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	fl	34685	US	www
12	[REDACTED]@aol.com	maria	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	ca	93060	US	hbwr
13	[REDACTED]@yahoo.com	maria	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]			US	limit
14	[REDACTED]@khalsa.com	sasha	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	co	80112	US	http;
15	[REDACTED]@yahoo.com	jenni	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]			US	yourg
16	[REDACTED]@yahoo.com	kristin	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	in	46307	US	buy.c
17	[REDACTED]@att.net	sherry	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	fl	32767	US	http;
18	[REDACTED]@aol.com	bob	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	ga	30013	US	123fr
19	[REDACTED]@msn.com	brianna	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	ca	90621	US	buy.c
20	[REDACTED]@carnegietechgroup.com	john	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	md	21035	US	entre
21	[REDACTED]@msn.com	elnora	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	mi	49426	US	www
22	[REDACTED]@juno.com	jason	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	oh	44223	US	enew
23	[REDACTED]@aol.com	christopher	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	sc	29464	US	myfr
24	[REDACTED]@comcast.net	willie	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	ga	30240	US	morn
25	[REDACTED]@juno.com	john	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	ca	95648	US	tagge
26	[REDACTED]@yahoo.com	natassha	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]			US	news
27	[REDACTED]@yahoo.com	sheniqua	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	ny	10475	US	ning.
28	[REDACTED]@netzero.net	shirrell	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	oh	44720	US	tagge
29	[REDACTED]@yahoo.com	chris	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	tn	38002	US	natio
30	[REDACTED]@peoplepc.com	bruce	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	ia	50060	US	work
31	[REDACTED]@netzero.net	cheri	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	il	62530	US	ning.
32	[REDACTED]@aol.com	tanishia	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	nc	28806	US	stude
33	[REDACTED]@msn.com	jason	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	ok	74108	US	rente
34	[REDACTED]@comcast.net	carlene	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	nh	3448	US	empl

A cooperative team of investigators from the MacKeeper Security Research Center, CSOOnline, and Spamhaus came together in January after I stumbled upon a suspicious, yet publicly exposed, collection of files. Someone had forgotten to put a password on this repository and, as a result, one of the biggest spam empires is now falling.

Additional coverage can be seen over at [CSOOnline](#).

The leaky files, it turns out, represent the backbone operations of a group calling themselves River City Media (RCM). Led by known spammers Alvin Slocombe and Matt Ferris, RCM masquerades as a legitimate marketing firm while, per their own



The screenshot shows a Microsoft Word document with a ribbon at the top containing Font, Paragraph, and Styles tabs. The document content is as follows:

Project X1 (IPv4/IPv6)

Summary

Project X1 is internally called "IPQ". It's written on top a set of Linux Kernel capabilities. It was written initially as a method of supplementing PowerMTA mail queue handling. It evolved into a full on IP state handling system. It's written and configured to maximize bulk delivery on IP resources. It is currently being used to send over 150 Million bulk messages per day to Yahoo across 3 servers. In 2013 an IPv6 version of "IPQ" was used across 4 servers to send over a billion bulk messages to Gmail per day, 18 Million inbox to Comcast in one day resulting in \$15,000 in revenue and 15 Million to AOL inbox in one day resulting in over \$21,000 revenue. This program has no GUI – because of its nature it runs from a Linux Console. Any sort of debugging requires Linux administration skills. Written in C++.

Highlights

- IP States, scores, and domain associated with each IP in our system are stored in Redis and are easily changeable.
- Estimated reputation level is based on a highly configurable 'scoring system'. Scores are added and deducted from each IP based on returning packets that come over the network from the target ISP mail servers.

Status

IPQ is used in production and is stable. The IPv6 version is also in stable working condition, but has not been used recently due to wavering IPv6 mailing opportunities. This platform serves currently as a revenue generator and has some unused features that will be extremely useful in the future with IPv6 email. This platform is well documented.

Think about that for a second. How can a group of about a dozen people be responsible for one billion emails sent in one day? The answer is a lot of automation, years of research, and fair bit of illegal hacking techniques. I say illegal hacking due to the presence of scripts and logs enumerating the groups' many missions to probe and exploit vulnerable mail servers. The following chat log,

found among the backups, is just one example of River City Media crew members admitting to exploitive behavior.

10:57

Sean: [...] then we're stuffing it into the kernel

Sean: waiting in a queue to process which is intentionally slow and fragr

Sean: so that we keep the connections alive but havent sent a single conn

Sean: then when they're all ready we stop fragging, remove the latency a
down their throats as possible until they disconnect you

In that screenshot, a RCM co-conspirator describes a technique in which the spammer seeks to open as many connections as possible between themselves and a Gmail server. This is done by purposefully configuring your own machine to send response packets extremely slowly, and in a fragmented manner, while constantly requesting more connections.

Then, when the Gmail server is almost ready to give up and drop all connections, the spammer suddenly sends as many emails as possible through the pile of connection tunnels. The receiving side is then overwhelmed with data and will quickly block the sender, but not before processing a large load of emails.

Purposely throttling your own machinery to amass open connections on someone else's server is a type of Slowloris attack

[[https://en.wikipedia.org/wiki/Slowloris_\(computer_security\)](https://en.wikipedia.org/wiki/Slowloris_(computer_security))]. The twist here is that the spammer is not trying to completely disable the receiving server, he is only temporarily stressing the resources in order to overwhelm and force the processing of bulk email.

Details of the even more abusive scripts and techniques have been forwarded on to Microsoft, Apple, and others. Law enforcement have also been notified and, while we are prohibited from saying too much, they are indeed interested in the matter.

1.4 Billion

Through offers such as credit checks, education opportunities, and sweepstakes, this spam operation has gathered and conglomerated a database of 1.4 billion peoples' email accounts, full names, IP addresses, and often physical address. There is evidence that similar organizations have contributed to this collection. An active market exists for trafficking in these types of lists for illegitimate purposes.

Imagine the privacy and legal implications here. Law enforcement agents normally have to go through a subpoena process before a service provider will hand over the name behind an IP address or account. This list maps out 1.4 billion.

The natural response is to question whether the data set is real. That was my initial reaction. I'm still struggling with the best software solution to handle such a voluminous collection, but I have looked up several people that I know and the entries are accurate. The only saving grace is that some are outdated by a few years and the subject no longer lives at the same location.

Random selections also consistently appear to reflect real people. Investigating

names from the list, through social media and work websites, usually shows that the additional details in the entry are most likely accurate. However, it's not so verifiable that a common web scraper could have easily gathered all the data.

Well-informed individuals did not choose to sign up for bulk advertisements over a billion times. The most likely scenario is a combination of techniques. One is called co-registration. That's when you click on the "Submit" or "I agree" box next to all the small text on a website. Without knowing it, you have potentially agreed your personal details can be shared with affiliates of the site.

You are never told who the affiliates are and groups like River City Media capitalize on that aspect. One line of the leaked chat logs explains it all very succinctly:

"The key is sincerity. Once you can fake that..."

Keep that line in mind if there is an official response from Alvin Slocombe, Matt Ferris, or one of the other River City Media crew members.

As of this morning, Spamhaus will be blacklisting RCM's entire infrastructure.

Alvin: <https://www.spamhaus.org/rokso/spammer/SPM1247/alvin-slocombe-cyber-world-internet-services>

Matt: <https://www.spamhaus.org/rokso/spammer/SPM1011/matt-ferris-river-city-media-acetech-usa>

Watch this blog for updates to the story as well as further details about the RCM operation. There are enough spreadsheets, hard drive backups, and chat logs here to fill a book.

Attention - Portions of this article may be used for publication if properly referenced and credit is given to MacKeeper Security Researcher, Chris Vickery.

Do you have security tips or suggestions?

Contact: cvickery@kromtech.com or security@kromtech.com

Stay tuned to the latest security news by visiting [MacKeeper Security Watch blog with Chris Vickery](#).

More Related Articles



Pet Retailer Still Leaking 110k+
Credit Card Details



AMP Trading Platform Breach



Schoolhouse Data Breach

0 Comments

MacKeeper Blog

 Login ▾

 Recommend **69**

 Share

Sort by Best ▾

Start the discussion...

Be the first to comment.

 Subscribe

 Add Disqus to your siteAdd DisqusAdd

 Privacy

DISQUS

Store

Company

EULA

Privacy Policy

Research Policy

© 2017 Kromtech Alliance Corp. All rights reserved.